I CLAIM:

1. A method for protecting electronic media, comprising:

encrypting the media;

transmitting the encrypted media – together with data indicating a first set of permissions – to a user device;

decrypting and using the electronic media at the user device in accordance with the first set of permissions;

sending a signal from the user device requesting additional permissions;

receiving at the user device data representing additional permissions; and

using the electronic media at the user device in accordance with the additional permissions.

2. In a method of delivering electronic content from a server to a user, and rendering the content with an application program, an improvement wherein the server:

computes a one-way hash function on data representing the content, yielding hash data;

encrypts data including the hash data; and

transmits the encrypted hash data to the user;

and wherein the application program:

checks the authenticity of the delivered content by reference to the encrypted hash data; and

refuses to render the content if said check fails.

3. The method of claim 2 in which the said encryption is performed using a key associated with said user.

4. A method for protecting electronic media, comprising:

storing encrypted media on a user device;

receiving a request to utilize the stored media in a first manner;

checking first license data on the user device to determine whether use of the stored media in the first manner is authorized; and if not:

contacting a remote server;

performing a licensing transaction with the remote server, resulting in issuance of second license data by the remote server;

storing the second license data on the user device; and

decrypting the media for use.

5. The method of claim 4 that includes, if said checking determines that use of the stored media in the first manner is not authorized, then informing the user of such fact prior to said contacting.

6. The method of claim 4 in which the remote server encrypts the second license data using a key associated with an intended licensee, and transmits the encrypted second license data to the user device.

7. A method of enhancing a content rendering application or a content authoring application, comprising:

receiving a rights management software development kit; and

modifying said application in accordance with software included in said kit, to thereby impart rights management functionality to said application.

8. A method of controlling use of a content object that includes text, the method including:

receiving data representing the object at a user device;

receiving at the user device an initial set of data representing usage rights associated with said object, the initial set of data defining a first set of rights that are permitted, and a second set of rights that are not permitted; and

upon receiving a request to perform a function using said content, checking said initial set of data representing usage rights to determine whether said function should be allowed, and

wherein a drag and drop function is among those that are not permitted.

9. The method of claim 8 wherein a modify function is among those that are not permitted.

10. The method of claim 9 wherein printing and saving functions are among those that are not permitted.

11. The method of claim 8 wherein the second set of rights is expressly defined in said data representing usage rights, rather than being inferred by their absence from the first set of rights.

12. The method of claim 8 wherein, if said check determines that said function should not be allowed, then engaging in a transaction with a remote server that results in receipt of revised data representing usage rights at the user device.

13. A method of controlling use of a content object that includes text, the method including:

receiving data representing the object at a user device;

receiving at the user device an initial set of data representing usage rights associated with said object, said data defining a first set of rights that are permitted, and a second set of rights that are not permitted; and

upon receiving a request to perform a function using said content, checking said data representing usage rights to determine whether said function should be allowed;

wherein a transmission function is among those that are not permitted.

14. A method of controlling email comprising:

receiving data representing email at a user device;

receiving at the user device an initial set of data representing usage rights associated with the email, the initial set of data defining a first set of rights that are permitted; and

upon receiving a request to perform a function using the email, checking said initial set of data representing usage rights to determine whether the function should be allowed,

wherein a transmission function is among those that are not permitted, and

wherein upon a blocked transmission, querying a remote server to determine criteria for transmission, and if the criteria is met, receiving an updated set of data defining a second set of rights that are permitted, the second set of rights including transmission rights.